MESSAGE TECHNOLOGY RESEARCH AND DEVELOPMENT

BOLT BERANEK AND NEWMAN, INCORPORATED,
CAMBRIDGE, MASSACHUSETTS

DECEMBER 1976

BBN REPORT NO. 3440

December 1976

MESSAGE TECHNOLOGY RESEARCH AND DEVELOPMENT

Quarterly Progress Report No. 3

2 July 1976 to 2 October 1976

PROJECT HERMES

Bolt Beranek and Newman Inc. 50 Moulton Street Cambridge, Mass. 02138

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER BBN REPORT NO. 3440	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) MESSAGE TECHNOLOGY RESEARCH AND DEVELOPMENT		5. TYPE OF REPORT & PERIOD COVERED Quarterly Progress 7/2/76 - 10/2/76
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) J. Burchfiel, T. Myer		8. CONTRACT OR GRANT NUMBER(s) MDA903 76 C 0212
9. PERFORMING ORGANIZATION NAME AND ADDRESS Bolt Beranek and Newman Inc. 50 Moulton Street Cambridge, Massachusetts 02138		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS		12. REPORT DATE December 1976
		13. NUMBER OF PAGES<br~~49 + iii~~ 53
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Distribution of this document is unlimited. It may be released to the Clearinghouse, Department of Commerce for sale to the general public.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

This research was supported by the Defense Advanced Research Projects Agency under ARPA Order No. 3161

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Hermes
Message Processing
Tenex Security
CINCPAC Test

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This report describes BBN efforts in the continuing development of the HERMES message-processing system, with respect to system design, security requirements and preparations for the DARPA/NAVY/CINCPAC interactive test.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

1 SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

BBN Report No. 3440 December 1976

MESSAGE TECHNOLOGY RESEARCH AND DEVELOPMENT

Quarterly Progress Report No. 3

2 July 1976 to 2 October 1976

This research was supported by the Defense Advanced Research Projects Agency under ARPA Order No. 3161 Contract No. MDA903-76-C-0212

TABLE OF CONTENTS

I. INTRODUCTION

This report covers progress in message technology under the contract "Message Technology Research and Development" for the period 2 July 1976 through 2 October 1976.

This work is a continuation of work on MAILSYS/HERMES performed under the ARPA Contract "Distributed Computation and TENEX Related Activities" during 1975.

During the July-September quarter, the primary effort of the HERMES project was directed toward preparation for the DARPA/NAVY/CINCPAC test (the Military Message Experiment or MME).

We completed the preliminary design of a multilevel secure environment for the CINCPAC version of the HERMES system and began work on a simulated demonstration version of CINCPAC-HERMES system. We continued the implementation of the interface between the HERMES system, running on the TENEX operating system, and the LDMX.

Our preparations for the MME also included the design and partial implementation of a facility for creating new types of message fields on demand, a facility for attaching comments to received messages, and a scope-oriented text editor suitable for use with the MME scope terminals. We implemented automatic programs for analyzing the statistics messages which are automatically generated by the HERMES System, and which were described in the previous progress report. These statistics can

be used in the MME and elsewhere to provide accurate information on HERMES usage.

Our secondary effort during this period was to extend the facilities of the generalized HERMES system in parallel with the developments required for the CINCPAC-HERMES system, and to make these facilities available to our users on the ARPANET and elsewhere. We also continued the development and improvement of other aspects of the HERMES system, such as documentation, output-device specification and the details of command structure, which will be of value to both the CINCPAC-HERMES users and the general user community.

User-Created and Comment Fields

The current set of HEADER fields in the HERMES Message system include several military-type fields which are rarely, if ever, used in informal messages. However, these fields are not sufficient for all types of military messages that may be encountered in the MME and other military applications. Many military groups, as well as users who want to use the HERMES system for office management and other specialized tasks, desire to create their own sets of individualized header fields.

For this reason, we began work on the design and implementation of User-created fields, which will allow a user or groups of users to tailor-make any number of message fields for any purpose. User fields will be of several different

data-types: One-line or multiline text fields, addressee fields, fields containing TENEX file names, fields containing dates, and numeric fields.

Another facility which many users desire is the ability to comment upon a received message and then either to refile the message or to send it on to someone else. We began implementation of Comment fields, which will be multi-line User-created fields. A Comment field will have a name that ties it to a specific primary field, and all Comment fields will become a part of the message to which they refer whether it is a received message or one previously created by the User.

The Scope Editor

The MME will make use of HP2640/45 Scope terminals. Since the text editors currently available in the HERMES system (TECO, XED and NETED) are not specifically designed as editors for scopes, and since no editor capable of exploiting fully the display capabilities of the HP2640/45 terminal was available, we completed the preliminary design and implementation of a new Scope Editor for text.

The new Scope Editor takes full advantage of the two-dimensional display capabilities of the scope, including a visible cursor that can be positioned to any point on the display screen. Corrections are made at the point specified by the cursor, and the text is shown in precisely the form that it will

have in the final version. For this reason, the editor has been named WE, which is short for the WYSIWYG or "What You See Is What You Get" Editor. WE allows the user to see the results of any text-editing commands much more quickly and directly than is possible with the current editors.

Two different keyboard command sets have been demonstrated, one using a function-key pad and the other using the ordinary keyboard in a command mode. The program is written modularly to allow experimentation with different terminals and different types of interaction between the terminal and the user.

The Experimental Encryption Facility

An experimental encryption facility was completed demonstrated. The encrypted text contains only ordinary alphabetic and numeric characters. Because this facility provides encryption but not true security of the type planned for the CINCPAC-HERMES System, the encryption commands will not at present be included in released versions of the HERMES System.

Statistics on Hermes Use

A program for analyzing statistics on HERMES usage was been implemented. Statistics were collected for more than 16,000 individual HERMES sessions, and a preliminary analysis was completed.

Security for the DARPA/NAVY/CINCPAC test

An important part of the effort of the HERMES project was focussed on meeting and security requirements for the DARPA/NAVY/CINCPAC test.

a) Applications-level security: The preliminary design of a multi-level secure environment for the CINCPAC version of the HERMES Message System was completed. Coding was completed for the simulated security system, and begun for the simulated "front-end" commands.

b) Host-to-Host Security: Design work was begun on the extension of the ARPANET TCP Protocols (rather than the NCP Protocols) for use in a multilevel secure environment. This work is reported as part of the packet Radio Project, and is therefore not included in this Progress Report.

The HERMES Incoming Message Processor

Implementation was completed except for the facility for handling priority messages. The design of the LDMX incoming message processor was partially reimplemented because of changes in the Navy protocols. Specification was begun for an interim magnetic tape interface between the LDMX and TENEX.

II. HERMES VERSION 2.6.6

A. DOCUMENTATION

1. HERMES Documentation Stored as HERMES Messages

NEWS since May 3, 1976, is now stored as a series of messages, one NEWS item to a message in a HERMES message-file. This arrangement takes advantage of the versatility of HERMES messages. When a new version of HERMES is released, the User can Survey the NEWS message-file and print out the individual NEWS items of interest, rather than having to read through a single long NEWS document. To see the NEWS message-file, use the HERMES command GET, e.g., for the BBN host computers, give the command

>Get <DOCUMENTATION>HERMES.NEWSMSG<CR>

The automatic initial survey prints surveys of all the NEWS items that you have not previously seen.

Similarly, a set of HERMES messages containing BASIC INSTRUCTIONS on how to use the HERMES System is stored in the message file <DOCUMENTATION>HERMES.INSTRUCTION.

2. Revised Documentation; New Reference Summary in DESCRIBE

A new interactive version of HELP introduces basic HERMES commands and guides you to other forms of documentation. DESCRIBE has been revised and updated.

A new, concise Reference Summary of all HERMES commands, with arguments and defaults, and with information on specifying sequences and about characters used in HERMES is available. Print it on the lineprinter or on the user's printing terminal:

```
>Describe Reference LPT:<CR>
     or
>Describe Reference<CR>
```

B. IMPROVED OUTPUT-DEVICE SPECIFICATION

1. "LDESTINATION"

For users who are physically remote from the lineprinter associated with their computer center, we have introduced a new object "LDESTINATION". LDESTINATION is the default destination for the LIST command.

The initial setting of LDESTINATION is LPT: = lineprinter. For users of the BBN systems, LPT: causes the output of the List command to be printed on the lineprinter located at 10 Moulton Street, Cambridge, Mass.

To change the LDESTINATION to TTY: = the user's terminal:

>Use LDESTINATION TTY:<CR>

2. Destinations in the Profile

Another new feature is that the EXPORT command now saves either the new LDESTINATION or the FDESTINATION permanently in the User's Profile.

>Export LDESTINATION<CR> [Replace old version]<CR>

C. IMPROVED DATE RECORDS

The Rcvd-Date field has been supplemented by a new message field named Filed-Date. Rcvd-Date is obtained from the "date stamp" that the TENEX File Transfer Portocol (FTP) places on the incoming message. Filed-Date is the most recent date on which the message was placed in its current message-file. The Rcvd-Date does not change when a message is filed in a new message-file, but the Filed-Date does change.

Formerly, the Rcvd-Date was changed whenever a message was transferred from one file to another with the FILE command. As a result, the standard survey template showed misleading dates in the Rcvd-Date field. Now the Rcvd-Date stays constant no matter how many times the message is Filed, but the Filed-Date determines whether a message has the attribute RECENT, i.e., whether it was placed in its current message-file since the last time the user entered that file.

Messages with an FCC:-field instead of addressee fields do not go through the MAILER program; however, the HERMES System itself creates a "Date Stamp," which acts as Rcvd-Date, when the message is sent.

D. NEW NETWORK ADDRESSING FACILITIES

The HERMES System now uses the Mail Forwarding Data Base (MFDB) to check addresses. At present, an active MFDB is implemented only on the five BBN systems. The MFDB provides improved address handling because it makes it possible to check the validity of user names on host computers other than the local host.

The HERMES System extends local names if you type the <ESC> key. After you type "," or "<CR>", HERMES checks with the MFDB and supplies the host name. If the name is local on your system, for example, if you are a user of BBNA and "Smith" is also on BBNA:

```
>To: Smi<esc>TH<CR>
>Show Typedform To<CR>
To: Smith at BBN-TENEXA
```

If Jones is on another host, say BBNE, and is listed in the MFBD, HERMES corrects the address, and notifies you of the correction.

```
>To: Jones, (= Jones at BBN-TENEXE)
```

A name with an explicit host, e.g., Jones at BBN-TENEXE, is checked, and corrected if necessary. If a name with an explicit host is not found in the MFDE, it is rejected if the host is local. If the host is not local, the MFDB notifies you and allows you to choose whether to attempt to deliver the message.

E. IMPROVED REPLY COMMAND

The REPLY command has been changed to provide consistently accurate algorithms for (a) creating the correct name and host for the To:-field of the REPLY message, even for unusual and nonstandard original messages, and (b) assigning correct host names to the automatic copies generated by the REPLY command.

The REPLY command now has a new subcommand "ExcludeMe" that allows the user to send automatic copies to other addressees in the original message but exclude himself. Another subcommand, whose action is independent of ExcludeMe, restricts automatic copies to the names in the To:-field of the original message.

1. Host Names Supplied Correctly

a) Replying to the From: and Sender: fields of the original message.

If the From:-field contains a address of the form "Name at Host", the Reply message is addressed to that address.

```
From: Smith at HOST
Reply message: To: Smith at HOST
```

If the From:-field contains more than one word, NOT in the form "Name at Host", Hermes ignores it and sends the Reply to the Sender:-field

```
Sender: Smith at HOST
From: Mary Smith
(Reply) To: Smith at HOST
```

If the From:-field contains one word only, Hermes sends the Reply to the Sender:-field with the From-field as an attention subfield.

```
Sender: Smith at HOST
From: Mary
(Reply) To: Smith at HOST (Attn: Mary)
```

b) Sending copies to the To:-and Cc:-fields of the original message.

If the To:-or Cc:-fields contain names without hosts, Hermes supplies the host-name from the From:-field, or if that does not contain a host-name, from the Sender:-field.

```
Sender: Smith at HOST
From: Mary
To: JMILLER at BBNA, Jones
(Reply) To: Smith at HOST (Mary)
(Reply) Cc: JMILLER at BBN-TENEXA, Jones at HOST
```

2. Subcomands Allow ToOnlyCopies, IncludeMe, ExcludeMe.

There is a major change in the options available, but some of these options are temporarily available only as subcommands to the Reply command.

a) Options available through the REPLY-COPIES Switch:

"Ask" -- Hermes first asks:
Copies to all To: addresses?
If NO<CR>, Hermes does not ask any more questions.
If YES<CR>, Hermes then asks:
Copies to all Cc: addressees?

"Yes" -- No change. Copies are sent to all names in the To:-and Cc:-fields.

"No" -- No change. The Reply message is sent only to the name in the From:-(or Sender:-) field.

b) Options available through subcommands to the Reply command. To invoke these subcommands, end the Reply command with ",<CR>" rather than "<CR>" alone. The subcommand prompt is the plus-arrow "+>".

```
>Reply ,<CR>
+>?
Copies
ToOnlyCopies
NoCopies
AskCopies
IncludeMe
ExcludeMe
Send
NoSend
AskSend
Erase
NoErase
Archive
```

NoArchive
<terminator> or <separator>: CR LF ESC SPACE
+>

+>ExcludeMe<CR>
Copies are sent to names in either the To: or the To: and Cc: fields but the sender of the reply is excluded.

+>IncludeMe
IncludeMe is the reverse of ExcludeMe, and cancels its action. The default setting is IncludeMe.

+>ToOnly<CR>
Copies are sent only to the names in the To: field.

+>AskCopies<CR>
+>Copies<CR>
+>NoCopies<CR>
These subcommands have the same effects as the different settings of the REPLY-COPIES Switch. The subcommands override switchsettings.

The other subcommands override the effects of the REPLY-SEND, SEND-ERASE and SEND-ARCHIVE switches.

+><CR>
Ends the subcommand mode and starts the action of the Reply command

F. PROJECTED USER-CREATED FIELDS AND ANNOTATION

Work was begun to extend the ability of the HERMES user to control the basic structure of HERMES messages by adding two new types of flexibility to message-creation: (1) the ability to create new Header fields, of several basic types, which have the full power and potential of the current set of fixed Header fields, and (2) the ability to attach comments to received messages in such a manner that (a) the comments are clearly differentiated from the original message and are automatically marked with the author of the comment and date that the comment was made, and (b) the comments become an integral part of the original message.

1. User-Created Message Fields

The current set of HERMES header fields is a selection of military type fields, several of which are rarely, if ever, used in informal message traffic. At the same time, these fields do not fit all military applications.

Now that the HERMES system is provided with powerful and convenient means of selecting messages according to the information content of the header fields, and of controlling the creation and printing of selected headers through the use of HERMES templates, the system is demonstrating great potential as a generalized data management tool.

Several experimental projects currently use HERMES messages as information storage and retrieval devices.

For example, the current HERMES documentation makes use of HERMES messages to display individual NEWS items to HERMES users and to provide a set of basic instructional messages.

In addition, we have begun to store suggestions from HERMES users, and reports of HERMES bugs and problems, in the form of HERMES messages. These are concise abstracts of original messages, in which two of the current, fixed header fields are used to record the date of the original suggestion and the current state of the action taken, e.g., as "FIXED" or "PENDING".

The ability of the HERMES system to select, store and sort sequences of messages will allow us to generate formatted reports by printing selected fields through HERMES templates.

To facilitate the creation of new Header fields, the present Header and Text:-fields were grouped into field types, and a new type of field was projected, which will accept a floating-point decimal number.

The user-created fields will be defined by associating with each unique new field name one of the following field types:

ADDR Address-field: Like the To:-field; expects a list of addressees, separated by commas. <CR> terminates field.

FILE File-field: Like the Fcc:-field; expects a list of TENEX file names, separated by commas. <CR> terminates field.

DATE Date-field: Like the Start-Date:-field; expects a single date. <CR> terminates field.

NUM Numeric-field: New field type; expects a single floating-point decimal number; this may be entered as a integer. <CR> terminates field.

LINE One-Line text field: Like the Subject:-field; expects ordinary text. <CR> terminates field.

TEXT Multi-line text field: Like the Text:-field (except that User-Created TEXT-typpe fields may be searched with Filters); expects ordinary text including <CR>'s. <CTRL-Z> terminates field.

Fields of the DATE and NUM type contain a single number or date only, and must therefore always be one-line fields.

Fields of the ADDR, FILE, and LINE types are one-line fields when they are created with the normal command:

><field-name> <contents> <CR>
Ex.: >Subject: This is a subject field. <CR>

Such nominal one-line fields may be converted to multi-line fields in one of the following ways:

a) Terminate the field with ",<CR>" rather than "<CR>". This allows you to type another line. The "," is not included in the field.

Ex.: >Subject: This is a ,<CR>
two-line Subject field <CR>

b) Repeat the command.

Ex.: >Subject: This is a <CR>
>Subject: two-line Subject field <CR>

2. Annotation or Comment Fields

HERMES users have long expressed a need to be able to perform the machine equivalent of "scribbling a note in the margin of" a message before filing it or forwarding it to another user. Although this is possible to a limited extent with the current Forward command, Users want to be able to retain the ability to search for information in the header fields of the original message, to comment upon individual fields of the original message, and to search for information in the comments themselves.

This comment facility is especially desired in military applications where messages normally go through a process of review and revision by two or more people before they are sent.

During the past quarter, we began to design and implement "Comment" or "Annotation" fields that can be associated with any field of a received message. To add Comment fields to a received message, the user will use the EXPLODE command to place the message in the MESSAGE-EDITOR, then create a field of the TEXT type by giving a command:

>>Comment <field name><CR>

Along with the comments of the user, the comment field will automatically supply the following information:

The name of the field commented upon.
The name of the person making the comment.
The date that the comment is made.

The new field will become part of the current draft message, and the revised draft message with its comment fields can be given a new Fcc:-or To:-field and sent to the user or to someone else.

G. OTHER IMPROVEMENTS

1. Message-No., Char-Count Fields Enlarged

The characters allotted to the template fields "Message-No." and "Char-count" have been enlarged to 3 and 5 characters, respectively, so that Survey lines will no longer become ragged when message-nos. go over 99 or messages are longer than 9999 characters.

2. "Deleted" Notices Consolidated

The notices for "DELETED" messages have been consolidated. If you attempt to PRINT, SURVEY or LIST a sequence that contains deleted messages, HERMES now prints the notice "Messages 3,27,45:56 are marked deleted." before printing the remaining (undeleted) messages in the sequence.

3. "@" and "at"Synonymous in Message Creation

"@" and " at " are now synonymous in message creation. When you type addresses into a To:-, Cc:- or Bcc:-field, you may now use "at" interchangeably with "@". NOTE: You must put a space before and after "at"; you may type "@" with or without spaces:

```
>To: Smith at BBNA, Jones @ ISI, Robinson@OFFICE-1<CR>
```

4. <CTRL-E> Queried in Text

The HERMES interrupt character, <CTRL-E>, now gives you a chance to recover when you are typing text into a message field. HERMES queries you:

```
Control-E typed.  Abort input of Text (or Addressees)?
```

If you have typed <CTRL-E> accidentally, you can answer N<CR> and continue with your work.

5. New Mail Notice Before Quitting

If you Quit HERMES and there is new mail in your INBOX, HERMES notifies you, then asks "Quit anyway?" Answer No<CR> to abort the Quit.

6. "SPELL" Program in Text

The TENEX program named "SPELL" is now available in the Draft Editor, for use with the Text:-field only.

```
>Spell<CR>
```

As with TECO, XED and NETED, we assume the User knows how to use SPELL before you invoke this command. (See the TENEX USERS' GUIDE (Jan 75 edition), page 173.)

7. Revised Spelling Correction for Commands and Objects

The experimental spelling corrector in HERMES has been toned down. It is still concerned about doubled letters and transpositions, but it is much less eager to make other kinds of corrections.

8. New Command "SUSPEND"

The new HERMES command Suspend has the same effect as typing the interrupt character <CTRL-C> at top command level. Hermes halts, and you can go back to the same state that you left, by typing the TENEX command "Continue" to the TENEX prompt "@". HERMES resumes with the CMESSAGE-FILE, the CMESSAGE, all objects and all outgoing message fields intact.

```
>Suspend<CR>
Suspending HERMES
@Continue<CR>
Resuming HERMES
>
```

If you do not continue, give the TENEX command "Reset".

```
@Reset<CR>
```

NOTE: The TENEX command "Reenter" has the same effect as "Continue" after SUSPEND, QUIT and EXIT, BUT "Reenter" MAY NOT be used after <CTRL-C>.

9. "JUMP-TO" Takes Beginning, End

You can now JUMP-TO two new symbolic positions, Beginning (Message No. 0) and End (LASTMESSAGE + 1). The Beginning and End positions allow you to JUMP-TO either end of the CSEQUENCE, and then use the single-character commands <LF> and to step your may through CSEQUENCE.

10. "VERSION" Takes Shortform, Longform, Everything

The VERSION command now takes an argument:

```
>Version <argument><CR>
>Version<CR> = Version SHORTFORM<CR>

where <argument> may be
SHORTFORM -- prints only the HERMES Herald.
LONGFORM -- adds all file names and activated options.
```

EVERYTHING -- adds the free storage report, maybe more. This form is of value in debugging the system.

11. "MAILSTAT" Takes Login, Connected

The MAILSTAT command now takes a directory argument:

```
>Mailstat <directory><CR>
>Mailstat<CR> = Mailstate LOGIN<CR>

where <directory> may be
LOGIN
CONNECTED
```

12. Profiles Automatically Updated

When a new version of HERMES is released, HERMES now rewrites your old Profile so that it is compatible with the new HERMES.

III. THE SCOPE EDITOR

The text-editing programs written for the TENEX operating system and currently available in the HERMES message editor are TECO, XED and NETED. These are designed primarily for use with printing terminals. For the MME, we wish to provide a scope-created editor that makes fullest use of the capabilities of the HP2640/45 scope terminals. We therefore designed and began implementation of an editor which has the following features available only on highly sophisticated display scopes:

a) A one-line "window" at the top of the screen contains information about editing modes and commands. The rest of the screen is devoted to the lines of text being edited.

b) There is a visible cursor, which shows the location where text is to be added or deleted. This cursor may be moved with editing commands to any point on the screen while the rest of the display remains fixed. The cursor may move in increments of characters, words or lines.

c) Changes made to the displayed text appear immediately, and leave the text in precisely the same form that it will have in the final version. For example, if the editor is set to "ERASE" mode, the cursor will appear to "gobble up" the characters to the right of the cursor, one by one. In "OVERWRITE" mode, each character typed replaces a character to the right of the cursor. In "INSERT" mode, characters

to the right of the inserted text are pushed to the right-hand end of the line and then "wrapped around" to form a new line.

This scope editor is usable either as a stand-alone editor called from the EXEC, or as an editor within the HERMES System.

When an editing session is complete, the scope editor either writes a new file (when used stand-alone) or returns the edited text to the HERMES System. The filename may be defaulted to the next higher version of the file used as input (if any).

A. "WHAT YOU SEE IS WHAT YOU GET"

The scope editor displays an accurate picture of a portion of the text which you are editing. Changes appear in precisely the same form as in the final version. That is: "What you see is what you get". Hence the editor has been given the name: the WYSIWYG Editor, or WE. Some consequences of the WYSIWYG philosophy are:

1) Tabs cannot be distinguished visually from spaces, and therefore tabs may not occur in the text which you are editing. However, tab-like functions can be provided through the ability to move a fixed number of spaces from the left-hand margin and insert text at that point.

2) Spaces to the right of the last word on a line are not distinguishable from no characters to the right of that word, and therefore each line is filled to the right margin with spaces. To save space in the file generated by WE, trailing spaces are discarded at the end of session. During an editing session, it is possible to move the cursor to any position on the Screen, regardless of whether or not visible characters are present. This allows unlimited freedom in format control and composing "white space."

3) Control characters are not visible, so they may not occur in the text you are editing.

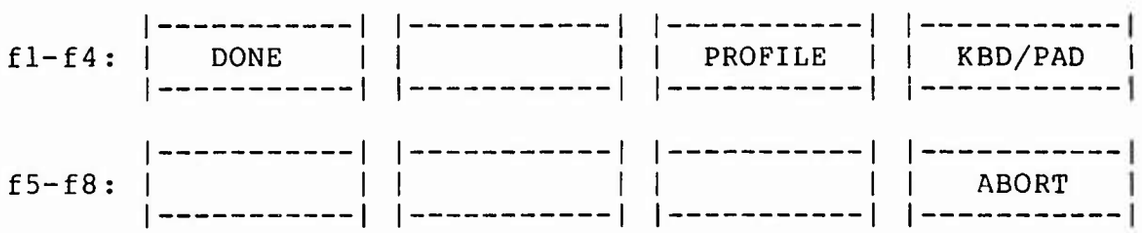
4) The screen has a fixed width, and therefore the lines in the text may have at a maximum that length. So-called "long lines" are not understood by WE. When text is inserted in a line, WE breaks the line of text at the spaces between words and carries over excess words to the next line, if there is room, to a new line. To save computing time, the ragged lines resulting from this type of insertion are not automatically evened up. Instead, the entire text field is formatted with the HERMES command Format after the editing with WE is completed.

The display presented by WE has two lines at the top which are used to contain information about the state of the editor and the text being edited. The remainder of the display is a view of a portion of that text. The cursor is used for indicating positions in the text.

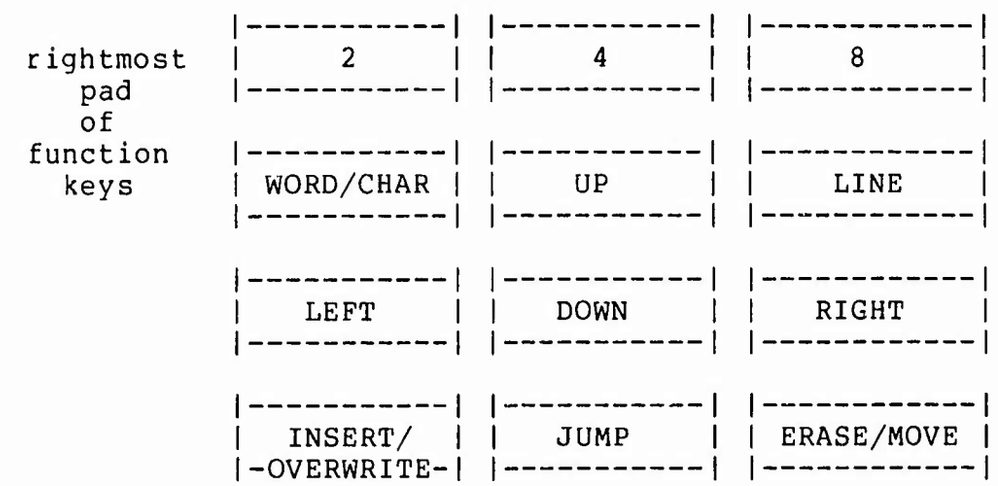
B. TEXT INSERTION AND EDITING FUNCTIONS

WE can be given commands in two ways: by typing characters, characters are added to the text; by hitting function keys, various editing functions are carried out.

The function key pads are arranged as follows:



Note: the CNTL key must be help down to get f1 and f8 to work.



The function keys are used to achieve the following functions:

UP or DOWN one line, no horizontal motion
LEFT or RIGHT,
one character (in CHARacter mode)
one word (in WORD mode)
to the end of the line
(hit LINE before LEFT or RIGHT)

The W/C function key switches between WORD and CHARacter mode.

Another function key switches between move and erase mode. In erase mode, all the motions just described are available: they have the effect of erasing those characters over which the cursor would have moved had you been in move mode.

The 2, 4 and 8 function keys are used for creating numbers, which are interpreted by WE as multipliers for its other actions. (For example, 2 4 RIGHT moves right 24 characters or words.)

There are two moves for adding characters to the text: either INSERT or OVERWRITE. The I/O function key switches between

these modes. In INSERT mode, characters to the right of the cursor are pushed to the right; when they hit the right margin, they are moved onto the next line (provided there is room) or onto a separate line which is inserted prior to the following line. In OVERWRITE mode, characters replace the characters indicated by the cursor.

The JUMP function key is used to jump to a different place in the text. The number function keys are used to indicate which line to jump to. (For example, 2 4 JUMP causes the cursor to be placed on line 24 of the text.)

The DONE function key is used to indicate that editing is finished. WE will then clear the screen and ask for an output filename.

The ABORT function key is used to indicate that editing is to be aborted; no output file will be written, or (when WE is used within Hermes) no change will be made to the field being edited.

The PROFILE function key is used to modify a collection of mode control switches which determine finer details of the way in which WE carries out the various actions descibed above. Hitting this key produces a display which explains the profile switches, their options, and how to change them. This is self-explanatory.

C. USE OF THE KEYBOARD FOR EDITING FUNCTIONS

One final function key is provided only for experimentation: the KBD/PAD key permits the keyboard to be used to invoke the editing functions associated with the function keys. When this key is hit, the functions associated with the function keys move into the keyboard. Thus, the LEFT function is invoked by typing L, RIGHT by R, and so on. Typing ESC changes the meaning of the keyboard from command to its "normal" meaning of letters to be added to the text. Hitting ESC when in this "KEYBOARD=KEYS" mode switches the mode back to "KEYBOARD=CMD". As a special aid, the I and O commands automatically switch from CMD to KEYS mode on the assumption that when you hit one of these you are intending to add characters to the text. [This mode is really intended for those who don't like function keys. If you like function keys, then this "multiplexing of the keyboard" is probably something you will never have to worry about much.]

The keys corresponding to the function keys are:

Ø-9	multiplexing numbers
W C	set WORD and CHAR mode (like toggling W/C)
U D	UP and DOWN
L R	LEFT and RIGHT
E R	set ERASE and MOVE mode (like toggling E/R)
I O	set INSERT and OVERWRITE mode (like toggling I/O)
%	JUMP
Q	DONE
H	ABORT
F	PROFILE
P K	set PAD and KBD mode (like toggling KBD/PAD)

Thus to get into KEYBOARD mode, the KBD/PAD function key is hit. To get out of KEYBOARD mode, the character P is typed in KEYBOARD=CMD mode.

D. ERROR-CORRECTION KEYS

There are a set of control characters which have also been implemented in WE to aid in correcting common typing errors:

ERASE CHAR LEFT
ERASE WORD LEFT
ERASE LINE LEFT
Repaint the screen (Helpful for when the HP scope gets confused; this is a common way to make sure that the picture is correct.)

IV. THE EXPERIMENTAL ENCRYPTION FACILITY

An experimental encryption facility has been designed and implemented, and is now running on an experimental version of the HERMES System. At present, there are no plans to include this facility in the standard HERMES System.

This encryption is based upon an existing BBN implementation of a National Bureau Standards encryption algorithm. (1) The original implementation, which is available as a TENEX program, produces a full range of ASCII characters, including control characters, in the encrypted text. Unfortunately, the control characters cannot be successfully transmitted over the network by the current version of MAILER, as people who have attempted to use it with HERMES or other message systems have discovered. We have designed the HERMES encryption facility to produce encrypted text consisting only of alphanumeric characters and other characters on the normal typewriter keyboard.

The HERMES commands ENCODE and DECODE operate upon the text in the TEXT field of the current unsent DRAFT message, and hence are available only in the MESSAGE EDITOR.

```
>Create<CR>
>>Text<CR>
This is a test message.
<CTRL-Z>
>>Encode<CR>
```

(1) Implementation by Paul Johnson, Bolt Beranek and Newman, Inc. The National Bureau of Standards algorithm is published as "Encryption Algorithm for Computer Data Protection", Federal Register, Vol. 40, No. 52, March 17, 1975, pp. 12134-12138.

```
key:  [HERMES]   Note: [...] indicates that the key
                 does not print on the terminal.
>>Show<CR>
5ox8w aj5va E#4If svaXO fkQRe #Wuf7 s3Mjb WTX2L Wv8QA Dvuz6
39jo8 5KBSg haPHf I7XXW 6p2Mq bYEEY EUaat ArQC8 caVns 936sH
JPfhW Z#1FØ WgXN6 oN7za Y####
>>Decode
key: [HERMES]
>>Show<CR>
This is a test message.
>>Encode
key: [MESSAGE]<CR>
>>Show<CR>
qhqHs bpV2R 4#ple R4hmG KQ3#w ysLØj i9ØZ8 lxsTV qG%Qw  i8AiC
QO818  RHRAv oqwgp kIclx CFawØ lcWcs SwrUØ inACH jt86Q 5msw2
QCeqC DiDCU rmVXF q3rtU 4####
```

The user can now add other message fields, send the message to someone else, and tell the recipient what the key is by some other means.

When the recipient receives an encoded message, he must use the EXPLODE command to place the text field of the received message in the text field of the unsent draft message.

```
>Survey 5<CR>
-+   5  483 SMITH AT BBN-TENEXA Encoded text field
>Explode 5<CR>
>>Show Text<CR>
qhqHs bpV2R 4#ple R4hmG KQ3#w ysLØj i9ØZ8 lxsTV qG%Qw i8AiC
QO818 RHRAv oqwgp kIclx CFawØ lcWcs SwrUØ inACH jt86Q 5msw2
QCeqC DiDCU rmVXF q3rtU 4####
>>Decode<CR>
key: [MESSAGE]<CR>
>>show<CR>
This is a test message.
```

If the key is wrong, the system prints an error message:

```
>>Decode<CR>
key: [MISSAGE]
? Decoding error -- wrong key given
```

V. STATISTICS ON HERMES USE

We collected statistics from just over 16,000 Hermes sessions during the period 8 June through 27 September, in the form of Hermes messages generated at the close of each Hermes session. These statistics currently record the top-level commands and the subcommands use to create messages. Analysis of these statistics messages was made with an automatic program which presented information for each weekly analysis period in the format shown in Table 1.

TABLE 1. FORMAT OF A STATISTICAL ANALYSIS REPORT

```
Sessions: <no. of sessions>
Av. real time: <time in seconds>
Av. think time: <time in seconds>
Av. computer time: <CPU time in milliseconds>

Command count/sess      real (sec)      cpu (millisec)
<Averages for each command used>

Av.s for msgs (<No. of messages>):
Addresses: <No. of addresses>
Length: <No. of characters>
```

The analysis yields the following information on the average behavior of the current group of HERMES users:

The average Hermes session lasted 21.4 minutes and consumed 20.2 CPU seconds. This suggests a long term average CPU rate for Hermes of just under one CPU minute per hour of connect time - 56.6 CPU seconds to be exact.

During the typical 21 minute Hermes session about 12 minutes were consumed in the execution of Hermes commands - entering messages into the system, printing them out, etc. During the remaining 9 minutes Hermes was idle; the user was presumably reading messages or deciding what to do next.

During the 16,000 sessions, slightly more than 8700 messages were created -- just over one message for every two Hermes sessions. It would appear that about half of all sessions are devoted to reading rather than sending mail.

These 8700 messages averaged 1427 characters in length (including headers); on the average, each message was sent to 3.4 recipients. Thus, counting each copy as a separate message, total traffic for the period was about 29,600 messages.

The weekly analyses generated by our current data reduction program are on file at Project Hermes, and can be made available to others, if desired. We can also supply the data reduction program and the message files of raw statistical data.

Analysis programs to operate on HERMES statistical data are easy to write. The contents of the different fields of the statistics messages can be extracted, by the use of Hermes templates, for input to the analysis programs.

EXAMPLE 1. A SAMPLE WEEKLY REPORT

Sessions: 1010
Av. real time: 971.7941 (sec)
Av. think time: 482.4713 (sec)
Av. computer time: 23053.44 (millisec)

Command	count/sess	real (sec)	cpu (millisec)
LF	0.90891	30.61	1785.3
PRINT	0.79901	169.31	7026.7
SURVE	0.50792	28.98	3926.9
Q	0.50495	4.30	612.3
QUIT	0.48416	7.22	384.7
DELET	0.46634	4.04	363.9
FILE	0.38020	16.89	1108.9
GET	0.37525	18.27	2841.9
COMPO	0.20495	476.56	4930.6
REPLY	0.19307	367.65	4815.6
S	0.19208	29.71	3517.9
CREAT	0.18812	386.61	5616.2
EDIT	0.14554	68.39	1321.0
SHOW	0.13366	19.84	1256.7
D	0.13168	5.25	326.4

STATU	0.12376	5.70	204.5
EXEC	0.11683	170.06	613.0
MOVE	0.11188	19.60	1582.2
LIST	0.10792	42.60	11707.1
FORWA	0.10000	140.81	5302.5
CNTO	0.08911	23.11	722.0
DESCR	0.06535	53.05	1199.3
DIREC	0.06040	17.69	1085.9
EXPUN	0.05644	7.04	1493.5
BSYS	0.05446	27.36	2012.6
CONSI	0.04653	8.51	1055.9
TRANS	0.04455	14.20	777.0
UNDEL	0.03465	3.86	326.4
ERASE	0.03267	7.61	220.5
MARK	0.02574	15.19	654.8
MAILE	0.02475	36.92	242.8
SUMMA	0.02178	39.68	7222.7
NEWS	0.01683	200.18	2876.0
MAILS	0.01584	35.06	1599.6
EXPLO	0.01584	385.56	7122.9
EXIT	0.01584	14.94	2736.0
UPAR	0.01584	8.56	843.1
CHECK	0.01188	7.58	743.5
USE	0.01089	101.73	263.2
COPY	0.00990	13.20	246.8
SUGGE	0.00792	234.13	3623.0
SEND	0.00792	96.50	2206.5
HELP	0.00693	467.43	9596.7
EXPOR	0.00594	8.00	667.0
JOBST	0.00594	5.83	698.0
DAYTI	0.00396	0.50	94.5
RETRI	0.00396	27.50	206.5
QFD	0.00297	48.33	1256.0
RUN	0.00099	6.00	82.0
IMPOR	0.00099	2.00	450.0
JUMP	0.00099	4.00	86.0
SEMI	0.00099	0.00	32.0
EXPLA	0.00099	59.00	1568.0

Av.s for msgs (495):
Addressees: 4.034343
Length: 1263.152 (chars)

VI. APPLICATIONS-LEVEL SECURITY FOR THE DARPA/NAVY/CINCPAC TEST

A. INTRODUCTION

We plan to provide CINCPAC with a message processing system which is very similar to the current HERMES System, but which supports CINCPAC operations and has the ability to operate in a secure environment.

This section describes a preliminary design for a set of modifications to the current HERMES System which we feel enables us to secure the system while still retaining its current "flavor" of operation.

The current HERMES System deals with messages (stored in TENEX message-files), drafts (of outgoing messages), templates, filters, and message sequences. In addition, the HERMES System has a "profile" for every user which includes the settings of certain switches governing the System's behavior, and any user-created filters or templates. We intend to keep the same basic view, but to extend it to include a notion of separate security levels.

When you use the CINCPAC HERMES System, it will appear to be a single HERMES program, very similar to the current one. The chief difference from the current HERMES System will be that the message-fields and other HERMES objects, such as templates, carry security-level labels.

You will be able to use all the functions of the current HERMES System to read and create messages and to create and modify such HERMES tools as sequences, filters, templates and switch settings. However, your access to the functions of the TENEX Executive program will be considerably more limited.

Once you have logged in at a given security level, you will be able to see all information at your security level or lower.

Before you create messages, you will be required to give special commands to get the security level of individual message-fields. All such fields must be at your security level or lower.

You may create two versions of the same message-field at two different security levels. As soon as you do, the CINCPAC-HERMES System, will engage in a dialog with you and require you to combine the versions into a single field and choose a single security level for it. If the fields are identical, CINCPAC-HERMES will choose the lower security level.

Throughout your HERMES session, you will be unaware of the existence of any part of the CINCPAC HERMES system at a security level above your login security level.

For example, a message in a CINCPAC-HERMES message file may contain an UNCLASSIFIED (U) Subject:-field and a TOP-SECRET (T) Text:-field. If you are logged in at any level below TOP-SECRET, this message will appear to have a Subject:-field but no

Text:-field and you will have no way of knowing whether or not a Text:-field exists. If you are logged in as TOP-SECRET, you will see both the Subject:-field and the Text:-field.

B. CONCEPTS UNDERLYING THE BBN SECURITY DESIGN

1. Use of the AIM Security Enhancements

We plan to run CINCPAC HERMES under the control of the AIM (1) security enhancements to the TENEX Monitor, to ensure that HERMES cannot accidentally cause a security breach.

2. The Job Structure

When you log into the CINCPAC-HERMES System, you will be required to state a security level. The CINCPAC-HERMES System will include a "Trusted Job" (TJ) which will act as the coordinator between the HERMES activities at different security levels.

The TJ, in turn, will create a separate and complete HERMES job at your security level and a partial HERMES job at each security level below your security level. Each "Security-Level HERMES Job" (SLHJ) operates independently. All communication between security levels will be through the TJ.

(1) S.R. Ames, Jr. and W.W. Plummer, "TENEX Security Enhancements", The MITRE Corporation,Bedford, Massachusetts, MITRE Technical Report, MTR 3217, Vol. 1. 1 April 1976 (ARPA F19628-76C-0001, 807B, D73)

However, you will not be aware of the TJ or the multiple SLHJ's. You will appear to be communicating with a single HERMES System which knows about security levels and which shows you all information at your security level or lower.

3. The Message Files

The CINCPAC-HERMES System will store messages in TENEX files. Each CINCPAC message file will appear to the user to be a single file, containing fields at different security levels. Actually, each CINCPAC message-file will consist of four TENEX message-files, one at each of the four security levels. Each Security-Level Message-File (SLMF) will contain only those portions of a message which are classified at the SLMF's security level. Therefore, in order to display the contents of a message, CINCPAC HERMES will examine the contents of all SLMF images of the message-file which are at or below its security level.

As in the current HERMES System, each SLMF image of the message-file will have a corresponding "parseg" or "curly-brace" file which contains parsing information created by the HERMES System.

4. The Outgoing Messages

Drafts of outgoing messages in the CINCPAC-HERMES System consist of a set of separate fields. Each SLHJ will have its copy consisting of fields at its security level only, but each

SLHJ will show the user all fields with a security level at or below its own.

5. The Objects: Sequences, Filters and Templates

Templates, sequences and filters in the CINCPAC-HERMES System will each exist at a specific security level, and be available to an SLHJ which is at or above that security level. To avoid conflicts of names, the security level will be included in the name. For example, a SECRET template would have a name like "TEMPLATE[S]".

6. The Operation of the "Trusted Job" (TJ)

The SLHJ will communicate with the TJ through a series of TENEX signals. When HERMES commands are passed from one SLHJ to another by the TJ, the CINCPAC-HERMES will require you to confirm them. Such commands will be stored in shared temporary files. Both the signals and the temporary files will be invisible to you.

The TJ will be called upon to perform its "functions" only when you give certain HERMES commands that involve more than one security level and hence would not ordinarily be permitted by AIM. For example, the HERMES command DELETE will requires the rewriting of all SLMF's which form a CINCPAC message-file and which are at or below your login security level. In order to

perform its functions, TJ must have both "Secure Write Down" and "Secure Job Start" capabilities provided under AIM.

7. The Security-Level Hermes Jobs (SLHJ)

If the action of the CINCPAC-HERMES System does not involve a change in security level, you will operate in one of the SLHJ created by the TJ.

Each SLHJ will be able to carry out some HERMES commands, including the creation of a fork under itself in order to run a scope editor or other program. Such a lower fork will always operate only at the security level of the SLHJ above it.

The SLHJ at your login security level will be able to carry out all commands available in CINCPAC HERMES. The SLHJ at lower security levels will carry out only the commands that cannot be carried out at your login security level.

C. THE USER INTERFACE TO A SECURE HERMES

1. Hermes Commands

The command language of the proposed CINCPAC HERMES System is nearly the same as that of the current HERMES. The principle differences are

1) There is a single EDITOR mode instead of separate editors for each type of object.

2) The new WE or "what-you-see-is-what-you-get" text editor (See Section III) designed especially for scopes is

automatically invoked when messages are created. The Scope-editor is also available for all other HERMES objects as an alternative to the specialized editing commands of the current HERMES System.

3) Several new commands are available that provide features not currently available in the current HERMES System (such as annotation).

4) Some existing commands are removed (such as EXEC, RUN, JOBSTAT).

5) Some of the current commands may take an extra argument. For example, CHECK-PRINTER, may take the name of the line printer that is to be checked).

6) Some commands are changed to include a security level.

When you log into the CINCPAC-HERMES System, you will be required to state your security level. The login command may take the form:

@LOGIN <user name> <password> <account no.> <security level><CR>

Once you have logged in, you no longer are able to get to the TENEX EXEC program, and you must logout directly from HERMES.

>Logout<CR>

When you see the ">" prompt, you are in the CINCPAC-HERMES System at your login security level and you have available most of the message-handling commands of ordinary a HERMES System.

As you work with incoming messages, you may change your message-file with the GET command, and SURVEY, PRINT or LIST messages at your security level.

2. The Editor Mode

The CREATE and EDIT commands have been condensed into one command, EDIT. The EDIT command prints out a notice of the security level and drops you into an editor mode with the distinctive prompt "=>".

```
>Edit <security level><CR>
                          where <security level>
                          defaults to UNCLASSIFIED
Security level: UNCLASSIFIED      [Inverse Video]
=>
```

At this point, you may either use message-creating subcommands to create or edit the outgoing message (CDRAFT), or you may enter one of the four object-editors

```
The SEQUENCE-EDITOR  with prompt "s=>"
The FILTER-EDITOR    with prompt "f=>"
The TEMPLATE-EDITOR  with prompt "t=>"
The SWITCHES-EDITOR  with prompt "sw>".
```

3. Creating Outgoing Messages

The "=>" subcommands in the Edit mode allow you to create or Edit message-fields at your login security level or at any lower security level.

Example: You are logged in as TOP-SECRET and wish to reply to a message that has a TOP-SECRET subject by creating a new message with a top-secret subject and UNCLASSIFIED text:

```
>Reply 7<CR>
To[U]: DODDS                Created automatically
Cc[U]: JMILLER              Created automatically
In-Reply-To[U]: <[CINCPAC]1-Jan-77 00:14:12.HOLLISTER>
                            Created automatically
Subject[T]: Re: Death in Venice
```

```
                                Created automatically
(Type text of Reply, to ^Z)
Text[T]: <CTRL-Z>^Z
                                Does not create Text: field.
=>UNCLASSIFIED<CR>
Security level: UNCLASSIFIED      [Inverse Video]
=>Text<CR>
That's too bad.<CTRL-Z>^Z
                                Creates  Text: field.
=>Show<CR>
To[U]: DODDS
Cc[U]: JMILLER

Subject[T]: Death in Venice
Text[U]:
That's too bad.
```

4. Creating and Editing Objects

When you want to use one of the object-editors, give either of the commands:

```
=>Create <object-type><CR>
      or
=>Get <object><CR>
```

Create and Get drop you into the appropriate editor for creating or editing a HERMES object. When you have finished, you can make a permanent copy of the new or edited object by using the new command SAVE.

The new HERMES subcommands TOP-SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED are available only in the top "=>" editor.

These commands allow you to change security levels for the purpose of creating message-fields or objects. However, you cannot create a message field or object at a higher security level than your login security level.

Example: You are logged in as TOP-SECRET. You have given the command:

```
>Edit TOP-SECRET<CR>
Security level: TOP-SECRET        [Inverse Video]
```

and you now wish to create an UNCLASSIFIED sequence.

```
=>UNCLASSIFIED<CR>
Security level: UNCLASSIFIED      [Inverse Video]
=>Create Sequence<CR>
s=>Add Subject: WEATHER<CR>
s=>Show<CR>
1,3,23:27,43,76
s=>SAVE WEATHER<CR>
[New Object: WEATHER[U]]<CR>
s=>Done<CR>
=>
```

This creates a new UNCLASSIFIED sequence named WEATHER[U] and permanently saves it.

Example: You wish to edit your CTEMPLATE but not to change its security level classification, which is CONFIDENTIAL.

```
>Edit CONFIDENTIAL<CR>
Security level: CONFIDENTIAL      [Inverse Video]
=>Get CTEMPLATE[C]<CR>
t=>Show<CR>
(1) To:
(2) Subject:
(3) [literal Keywords: Confidential Weather Project]
(4) Text:
t=>line-insert 2<CR>
literal Cc: JONES <CTRL-Z>^Z
t=>Show<CR>
(1) To:
(2) [literal Cc: JONES]
(3) Subject:
(4) [literal Keywords: Confidential Weather Project]
(5) Text:
t=>SAVE<CR>
[Replace old version: CTEMPLATE[C]]<CR>
```

This permanently saves a new copy of your CTEMPLATE at security level CONFIDENTIAL.

When you GET an object, the object must exist at a security level which is either at or below the level specified in the EDIT command. An object may be SAVED only at the current security level of the EDITOR.

D. SECURITY ASPECTS OF THE BBN TERMINAL DESIGN

The implementation will make use of two function keys: a CONFIRM key and a NO-CONFIRM key. There will also be four SECURITY-LEVEL letters designated as keys for the TJ.

In addition, on the terminal there will be a set of SECURITY LIGHTS for indicating the security level at which CINCPAC HERMES is currently operating.

Either the terminal or the TENEX monitor will be modified so that:

1) Commands to the terminal to retransmit the contents of the screen will be blocked, and hence cannot be used by CINCPAC HERMES.

2) The command to change the SECURITY LIGHTS and to turn on the Inverse Video will be sent only if the process sending the command has the "Secure Job Start" capability.

E. FUNCTIONS OF THE TRUSTED JOB (TJ)

1. Categories of TJ Functions

The TJ functions are "commands" or "calls" that the CINCPAC-HERMES System gives to the TJ. You never see these functions directly, but they cause actions that affect you in one of two different ways:

1) No User Interaction

   The CINCPAC-HERMES System requests the TJ to suspend operation of the current SLHJ and move to another SLH job at a different security level to perform a specific function. The TJ alerts you by changing the SECURITY LIGHTS on the terminal but does not require confirmation.

2) User Interaction

   The CINCPAC HERMES requests the TJ to pass information from a SLHJ at one security level to another SLHJ at a lower security level. The list of these functions is small, and each passes enough information to the TJ to allow the TJ to interact with you at your level. Normally, the TJ will simply print out a rephrasing of your previous command and await confirmation. Although the "flavor" of the interaction is different, these commands are similar to the commands in the current HERMES System which require double confirmation.

   Example:

   =>DELETE 5<CR>

   The TJ types out:

   {DELETE 5}:

   and waits for you to hit the CONFIRM key or the NO-CONFIRM key.

2. List of TJ Functions

1) "Start" (No User Interaction)

   Called after you log in. Creates HERMES jobs at all

security levels at and below your security level. The Start Function passes to each SLHJ the security level at which that the SLHJ will run, the level at which you logged in, and the job number of the TJ; it also sets up a signal between the TJ and the SLHJ.

2) "Request" (User Interaction)

The SLHJ passes a HERMES command string to the TJ. The TJ redisplays it, and then (if you confirm the command) outputs it to a temporary file at each security level. The SLHJ at that security level then reads the temporary file and executes the command, then deletes the temporary file.

The following HERMES commands act under the TJ "Request" function:

Top-Level Commands:
>Delete <sequence><CR>
>File <sequence> <file-name><CR>
>Forward <sequence><CR>
>Get <file-name><CR>
>Move <sequence> <file-name><CR>
>Reply <message-no.><CR>
Editor-Mode Commands:
=>Compose<CR>
=>Get <message-no.><CR>
=>Erase <All><CR>
=>Forward <sequence><CR>
=>Reply <message-no.><CR>
=>Include <message-no.><CR>
=>Restore-draft <file-name><CR>
=>Store-draft <file-name><CR>

3) "Force Single Version" (User Interaction)

The SLHJ passes a temporary file name to the TJ, and the TJ looks to see whether the temporary file name exists at another security level. If so, the TJ prints out the name of the temporary file and the security levels at which it exists. The TJ then starts a dialog:

{Subject[T] and Subject[U] exist.}
Combine them?}:
CONFIRM/NO-CONFIRM
ifCONFIRM
{Which one is first (T or U)?}: T/U

ifNO-CONFIRM
{Which is the final version (T or U)?}: T/U
{What is the security classification (T, S, C or U)?}:
T/S/C/U

If the final security level is lower than the maximum security level of the component fields, and if the resulting field is more than one page long, the field is shown to you one page at a time, and you are required to confirm each page.

If you want to start the dialog over again at any point, hit the NO-CONFIRM key.

4) "Move to security level <X> and enter the Editor" (No User Interaction)

This function tells the TJ to change the SECURITY LIGHTS on th terinal (thereby informing you of the security level change) and to detach the current SLHJ and attach the terminal to the SLHJ at the security level <X>. The TJ also sends a signal to the SLHJ at level <X> telling it to enter the EDITOR.

5) "Move to top security level and accept commands" (No User Interaction)

This function tells the TJ to change the SECURITY LIGHTS to your login security level and to attach the termirminal to the SLHJ at that security level. It also sends a signal to that SLHJ telling it to return to top-level command input.

6) "Send" (User Interaction)

This function is called when CINCPAC HERMES tries to send a message. The TJ actually does the sending.

7) "Logout" (No User Interaction)

This function is called after you tell CINCPAC HERMES to logout. It tells all of the SLHJ to perform any necessary clean-up operations, and then logs them out. Then the TJ logs out.

F. IMPLEMENTATION PLANS

1. Simulated Security for November

The simulated CINCPAC-HERMES System that BBN will demonstrate in November 1976 will differ from the final CINCPAC-HERMES System in two important ways:

1) The multipart CINPAC message-file, consisting of four separate security-level message-files (SLMF's) will be simulated by one TENEX message-file.

2) The multipart CINCPAC HERMES job, consisting of a Trusted Job (TJ) and one to four Security-Level HERMES Jobs (SLHJ's) will be simulated by one HERMES job.

The method of simulation will be to label each message-field and each HERMES object (sequence, filter or template) with a security label. The label will become part of the name of the field or object, so that it will be possible to create two objects with the same name at two different security levels.

Security rules will be enforced by code, with the aide of the HERMES System in interpreting the labels on the fields and objects.

2. Implemented Security for July 1977

The CINCPAC-HERMES System provided by BBN for the July 1977 CINCPAC Test will contain full implementation of multilevel CINCPAC message-files and multilevel HERMES jobs.

VII. THE HERMES INCOMING MESSAGE PROCESSOR

The design of the LDMX incoming message processor was changed during this quarter, due to protocol changes initiated by the Navy in the area of error handling. The redesign of the translator between the incoming LDMX messages HERMES messages has been completed. The re-implemetation is complete except for the handling of Priority messages.

The software for the LDMX, which is being produced by NAVCOSSACT has been delayed, necessitating the development of a interim system which can input messages into the TENEX system in the near future and can thereafter act as a back-up system. We have designed a magnetic tape system that records messages from the LDMX. These messages are then loaded into the TENEX system as input for the HERMES system. Specification is complete for the format in which the LDMX messages are recorded on the magnetic tape.

VIII. HUMAN FACTORS

The Human Factors Group prepared a draft of a protocol for the Military Message Experiment Organization Impact Study. This consists of a large set of candidate questions for the organization impact questionnaire which is being prepared in collaboration with MITRE and NAVSEA personnel.

We advised MITRE, NAVSEA and NAVELEX on manpower and organizational-impact input to the Military Message Experiment (MME) test plan.

We began work on a framework for predicting the organizational impact of DISTAN on Naval message processing operations.